

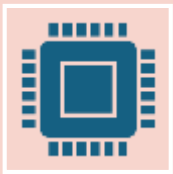
SDE 458 Senior Design Project

Using Virtual Machine's to
simulate and educate phishing
attacks in the workplace

By: Faith Olajide

April 10, 2024

Introduction and Background



Phishing attacks in the workplace are on a rise and have cost companies millions of dollars yearly. This not only causes monetary loss but also important data loss.



To combat this, my project will help educate and train employees on what phishing is, how to differentiate between a real email and a malicious one, and how to mitigate a phishing attack if one accidentally interacts with the email using virtual machines to simulate a phishing attack and a training module for employees.

Problem Statement

- Despite the numerous advancements in cybersecurity awareness, companies still face threats from phishing attacks, which are still a primary source of monetary loss and data breaches. Standard cybersecurity training practices frequently lack accuracy and fail to properly prepare employees to recognize and respond to phishing attempts. To mediate this, an accurate and thorough training program that uses virtual machines (VM) software to simulate real world phishing scenarios and give staff members hands-on training in a secure setting is required to meet this problem.

Required Materials

- Virtualization software: VMWare, Parallels, VirtualBox.
- Virtual Machines: Kali Linux, Email server
- Phishing Simulation Software: SEToolkit in Kali Linux
- Phishing Templates: Email template in SEToolkit and template created by student.
- Training Materials: Educational modules for employees
- User Guides/Policies and procedures
- Monitoring and Reporting Tools
- Security Measures for VMs
- Support and Training

What is Phishing and How does it work?

- Phishing is a social engineering attack that tricks people into giving out their personal information (credit card information, passwords etc.) by posing as a trustworthy source like a bank.
- It is usually done through email or social media.
- It works by an attacker sending messages that look legitimate to an unsuspecting person.
- Messages usually contain malicious links.

What to look for


- Messages will ask for personal information such as passwords or credit card information.
- Messages will create a sense of urgency to the target.
- Messages will come from an email address that appear legitimate but are spoofed.
- Messages may include links or attachments that lead to websites that look legitimate but are malicious.

Budget

Item	Description	Cost
Virtualization Software	VMWare vSphere Essentials Kit (1 year License)	\$500
	VirtualBox (Open Source)	\$0
	Parallels Desktop for Mac	\$59.99
Virtual Machines (VMs)	Kali Linux	\$0
Phishing Simulation Software	Phished.io, SEToolkit in Kali Linux	\$0
Training Materials	Youtube	\$0
Administration Costs	Eset	\$1625
Miscellaneous	Additional Software Licenses	\$500
Total		\$2,684.99

Project Schedule

	Activity	Description	Due Date	Comments
Week 1-2	Project Kickoff	Objectives are defined, met with professors about project.	1/12/2024	Initial project meeting was held, talked with professors to get ideas on how to execute project.
Week 3-4	Research on Virtual Machines	Research and requirement analysis	1/26/2024	Researched which virtual machine would be best to use for project.
Week 5-6	Scenario Development	Created a realistic phishing scenario for a company/organization	2/8/2024	Spoke to professors about project and did research on the best scenario.
Week 7-8	Virtual Machine Setup	Purchase and setup virtual machine for use	2/22/2024	Purchased Parallels and installed necessary software.
Week 9-10	Performed Phishing Simulation	Performed phishing simulation in Kali Linux	3/7/2024	Ran into a problem with Gmail security accepting third party account. Problem was fixed after thorough research
Week 11-12				
Week 13-14	Final Testing and Documentation	Performed final testing in Kali Linux	3/28/2024	Testing went smoothly with no errors. Training practices were prepared
Week 15-16	Training Module Created	Created several practices and policies to be implemented.	4/8/2024	Designed and refined training practices for company.



Phishing Simulation

Discussion

- One problem I faced was Google's security system would not allow the usage of third-party applications. This was solved by using a different SMTP server to send the email after careful research.
- My project is a hands-on training module that consists of the simulation on a virtual machine and a training module on a website.
- Applicability: cybersecurity preparedness, employee training, compliance, scalability, cost-effectiveness, and industry relevance.

Results

- Phishing simulation test was a success
- Software sent emails in a timely manner and was easy to learn/program.
- Only ran into one problem.
- Overall, the results of the project were a success

Results cont

Email address
is not legit.

New Update Inbox x



IT Department <faitholajide1@266106310.t-sender-sib.com>

Fri, Apr 12, 9:11 PM (2 days ago)



to me ▾

There was a new update to the overall document that I need you to review. You'll notice the changes on page 2 and 3.

Thanks for the help!

James

Suspicious
file
attachment

One attachment • Scanned by Gmail ⓘ



↩ Reply

➦ Forward



Training Module

- Goals: Train and educate employees on phishing practices.
- Execution: Will be done through a website called Knowbe4.
- Website will test employees on how phish prone they are and teach them how to not be phish prone.

Conclusion

- The project would have a positive impact in the field of cybersecurity because it would provide the necessary training for employees when it comes to phishing while saving companies money, time, and prevent data loss.
- It will allow employees to contribute to the industry by applying newfound skills and practices.
- I learned how phishing can impact the workplace and employees need proper training to mediate this issue.

References

- Brown, L. (2018). Challenges in Simulating Workplace Vulnerabilities with Virtual Machines. *Journal of Cybersecurity Research*, 6(3), 112-128.
- Chen, S. (2017). Cybersecurity Simulation: A Comprehensive Review. *International Journal of Information Security*, 15(3), 149-167.
- Johnson, A. (2019). Virtual Machine-Based Training for Cybersecurity Personnel. *Cybersecurity Education Journal*, 8(1), 78-92.
- Garcia, R. (2021). Virtual Environments for Identifying and Resolving Workplace Vulnerabilities. *Journal of Cybersecurity Practices*, 14(4), 205-220.
- Miller, P. (2016). Virtualization Technologies in Cybersecurity Education. *Journal of Educational Technology*, 10(2), 89-104.
- Phishing. IT Governance. (n.d.). <https://www.itgovernance.co.uk/phishing>
- Smith, J. (2020). Enhancing Cybersecurity through Virtual Machine Simulations. *Journal of Cybersecurity*, 12(2), 45-63.